

Family list

1 family member for:

JP2001249941

Derived from 1 application.

**1 DATA BASE ACCESS CONTROL METHOD, DATA BASE DEVICE AND
RECORDING MEDIUM HAVING DATA BASE CONTROL PROGRAM
RECORDED THEREON**

Publication info: **JP2001249941 A** - 2001-09-14

Data supplied from the **esp@cenet** database - Worldwide

THIS PAGE BLANK (USPTO)

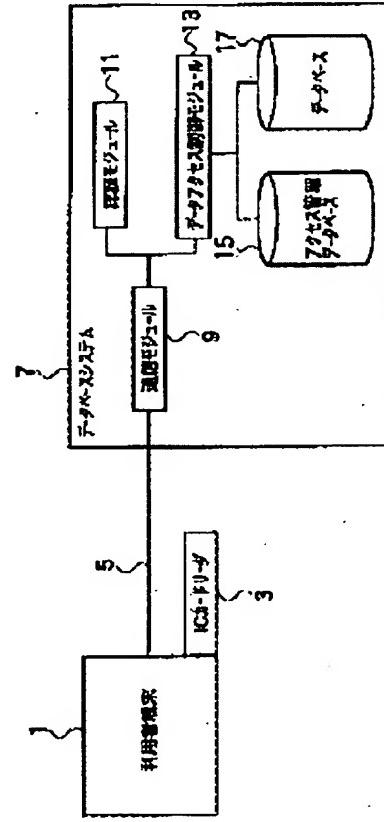
DATA BASE ACCESS CONTROL METHOD, DATA BASE DEVICE AND RECORDING MEDIUM HAVING DATA BASE CONTROL PROGRAM RECORDED THEREON

Patent number: JP2001249941
Publication date: 2001-09-14
Inventor: SUDO TOMOKO; KUBOTA YUKIHIRO; TSUBOI TOSHIAKI; NAKAMURA YOSHIAKI; HASHIMOTO SATOSHI; SAWACHI MAMORU
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
 - **international:** G06F17/30; G06F12/00; G06F12/14; G06F15/00
 - **european:**
Application number: JP20000060985 20000306
Priority number(s): JP20000060985 20000306

[Report a data error here](#)

Abstract of JP2001249941

PROBLEM TO BE SOLVED: To provide a data base access control method, a data base device and a recording medium having a data base control program recorded thereon capable of accurately preventing the leakage of the data of a data access object by using both of first authentication information for authenticating an accessing person like a doctor for instance and second authentication information for authenticating the data access object like a patient. **SOLUTION:** The first authentication information is transmitted from a terminal to a data base, the data base authenticates the authentication information and returns an authentication result to the terminal. The terminal transmits the second authentication information to the data base together with data specifying information. The data base authenticates the authentication information, judges the propriety of access to the data specified by the data specifying information on the basis of the authentication result and the data specifying information and permits the access to the data specified by the data specifying information in the case that the access is approved.



Data supplied from the **esp@cenet** database - Worldwide

PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-249941

(P2001-249941A)

(43)公開日 平成13年9月14日 (2001.9.14)

(51)Int.Cl. ⁷	識別記号	F I	デマコード(参考)
G 06 F 17/30	1 2 0	C 06 F 17/30	1 2 0 B 5 B 0 1 7
	1 1 0		1 1 0 F 5 B 0 7 5
12/00	5 3 1	12/00	5 3 1 A 5 B 0 8 2
12/14	3 1 0	12/14	3 1 0 K 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 D

審査請求 未請求 請求項の数11 O L (全 16 頁)

(21)出願番号 特願2000-60985(P2000-60985)

(22)出願日 平成12年3月6日 (2000.3.6)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 須藤 朋子

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社内

(72)発明者 久保田 幸宏

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社内

(74)代理人 100083806

弁理士 三好 秀和 (外1名)

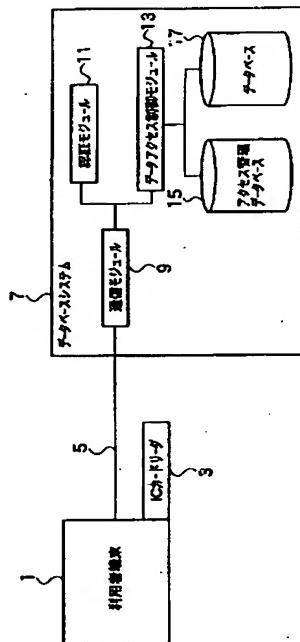
最終頁に続く

(54)【発明の名称】 データベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体

(57)【要約】

【課題】 例えば医師のようなアクセス者を認証する第1の認証情報と患者のようなデータアクセス対象を認証する第2の認証情報の両認証情報を用いて、データアクセス対象のデータの漏洩を適確に防止し得るデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体を提供する。

【解決手段】 端末から第1の認証情報をデータベースに送信し、データベースは該認証情報を認証し、認証結果を端末に返送し、端末はデータ指定情報とともに第2の認証情報をデータベースに送信し、データベースは該認証情報を認証し、該認証結果とデータ指定情報に基づきデータ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、データ指定情報で指定されるデータへのアクセスを許可する。



【特許請求の範囲】

【請求項1】 端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、
端末からアクセス者を認証する第1の認証情報をデータベース装置に送信し、
データベース装置は受信した第1の認証情報を認証して、その認証結果を端末に返送し、
端末は受信した認証結果に基づき所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともにデータアクセス対象を認証する第2の認証情報をデータベース装置に送信し、
データベース装置は受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを特徴とするデータベースアクセス制御方法。
【請求項2】 端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、
端末からアクセス者を認証する第1の認証情報およびデータアクセス対象を認証する第2の認証情報をデータベース装置に送信し、
データベース装置は受信した第1の認証情報を認証して、第1の認証情報と第2の認証情報を対にして格納し、
端末から所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信し、
データベース装置は受信した第1の認証情報で前記格納された第1および第2の認証情報の対を参照し、前記受信したデータアクセス対象が第1の認証情報に対して対として格納されている第2の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを特徴とするデータベースアクセス制御方法。
【請求項3】 前記データ指定情報で指定されるデータへのアクセスの可否を判定する処理は、該データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納していることを特徴とする請求項1または2記載のデータベースアクセス制御方法。

タベースアクセス制御方法。

【請求項4】 前記端末からアクセス者を認証する第1の認証情報をデータベース装置に送信する処理は、ICカードに格納されている第1の認証情報を読み出してデータベース装置に送信し、
前記端末からデータアクセス対象を認証する第2の認証情報をデータベース装置に送信する処理は、ICカードに格納されている第2の認証情報を読み出してデータベース装置に送信することを特徴とする請求項1または2記載のデータベースアクセス制御方法。

【請求項5】 端末は、前記データ指定情報で指定されるデータへのアクセスを許可された場合、該データ指定情報で指定されるデータに対するデータの変更、追加登録、読み出しを行うことができる特徴とする請求項1または2記載のデータベースアクセス制御方法。

【請求項6】 端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第1の認証情報を受信して認証し、この認証結果を端末に返送する認証手段と、

端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第2の認証情報を受信し、この受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを特徴とするデータベース装置。

【請求項7】 端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第1の認証情報をおよびデータアクセス対象を認証する第2の認証情報を受信し、この受信した第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納する格納手段と、

端末からデータを指定するデータ指定情報とともに送信されてくる第1の認証情報およびデータアクセス対象情報を受信し、この受信した第1の認証情報で前記格納手段に格納されている第1および第2の認証情報の対を参照し、前記受信したデータアクセス対象が第1の認証情報に対して対として格納されている第2の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを特徴とするデータベース装置。

【請求項8】 前記アクセス許可手段は、前記データ指定情報に対応して該データへのアクセスを許可するア

セス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを蓄積する蓄積手段を有することを特徴とする請求項6または7記載のデータベース装置。

【請求項9】 端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、
端末から送信されるアクセス者を認証する第1の認証情報を受信して認証し、この認証結果を端末に返送し、
端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第2の認証情報を受信し、この受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、
アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可することを特徴とするデータベース制御プログラムを記録した記録媒体。

【請求項10】 端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、
端末から送信されるアクセス者を認証する第1の認証情報をおよびデータアクセス対象を認証する第2の認証情報を受信し、この受信した第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納し、
端末からデータを指定するデータ指定情報とともに送信されてくる第1の認証情報をおよびデータアクセス対象情報を受信し、この受信した第1の認証情報で前記格納されている第1および第2の認証情報の対を参照し、前記受信したデータアクセス対象が第1の認証情報に対して対として格納されている第2の認証情報で認証されるものであるか否かを判定し、
該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報を前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可することを特徴とするデータベース制御プログラムを記録した記録媒体。

【請求項11】 前記アクセスを許可する処理は、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納することを特徴とする請求項9または10記載のデータベース制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、端末からデータベ

ース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体に関し、特に医師のICカードを使用して医療用データベース装置に接続し、患者のICカードを使用して医療用データベース装置に格納されている患者のデータに対してアクセスするデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】 患者のデータを格納した医療用データベースへのアクセスは、従来、医師のICカードのみで認証を行い、この認証結果に基づいてデータベースへのアクセス管理を行っている。

【0003】 すなわち、この種のデータベースは、従来、医師会所属の医師または系列病院の医師のみの使用を目的として構築されているが、今後病診連携や地域医療が進むと、より多くの医師が患者のデータにアクセスする必要が出てきて、同じ患者のデータに対してより多くの医師のアクセスを許す必要が出てくることになるため、患者データの漏洩対策を考慮する必要がある。しかしながら、従来のように医師のICカードのみの認証によるデータアクセス制御では患者データの漏洩時の責任を明確にすることはできない。

【0004】

【発明が解決しようとする課題】 上述したように、病診連携や地域医療が進んで、より多くの医師が患者のデータにアクセスし、同じ患者データに対してより多くの医師のアクセスを許すことになると、従来のように医師のICカードのみの認証によるデータアクセス制御では患者データの漏洩時の責任を明確にすることはできないという問題があり、医師のICカードの認証結果と患者のICカードの認証結果の両方を用いて、より細かく、安全なデータアクセス制御を行い、患者データの漏洩対策を適確に行う必要がある。

【0005】 本発明は、上記に鑑みてなされたもので、その目的とするところは、例えば医師のようなアクセス者を認証する第1の認証情報と患者のようなデータアクセス対象を認証する第2の認証情報の両認証情報を用いて、データアクセス対象のデータの漏洩を適確に防止し得るデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体を提供することにある。

【0006】

【課題を解決するための手段】 上記目的を達成するため、請求項1記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、端末からアクセス者

を認証する第1の認証情報をデータベース装置に送信し、データベース装置は受信した第1の認証情報を認証して、その認証結果を端末に返送し、端末は受信した認証結果に基づき所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともにデータアクセス対象を認証する第2の認証情報をデータベース装置に送信し、データベース装置は受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを要旨とする。

【0007】請求項1記載の本発明にあっては、端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第2の認証情報をデータベース装置に送信し、データベース装置は第2の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。

【0008】また、請求項2記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、端末からアクセス者を認証する第1の認証情報およびデータアクセス対象を認証する第2の認証情報をデータベース装置に送信し、データベース装置は受信した第1の認証情報を認証して、第1の認証情報と第2の認証情報を対にして格納し、端末から所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信し、データベース装置は受信した第1の認証情報を認証する第2の認証情報をデータアクセス対象が第2の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを要旨とする。

とを要旨とする。

【0009】請求項2記載の本発明にあっては、端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して、第1の認証情報と第2の認証情報を対にして格納し、端末からデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第1および第2の認証情報の対を参照し、データアクセス対象が第2の認証情報で認証されるものであるか否かを判定し、そうである場合、第1、第2の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行なうことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【0010】更に、請求項3記載の本発明は、請求項1または2記載の発明において、前記データ指定情報で指定されるデータへのアクセスの可否を判定する処理が、該データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納していることを要旨とする。

【0011】請求項3記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【0012】請求項4記載の本発明は、請求項1または2記載の発明において、前記端末からアクセス者を認証する第1の認証情報をデータベース装置に送信する処理が、ICカードに格納されている第1の認証情報を読み出してデータベース装置に送信し、前記端末からデータアクセス対象を認証する第2の認証情報をデータベース装置に送信する処理が、ICカードに格納されている第2の認証情報を読み出してデータベース装置に送信することを要旨とする。

【0013】請求項4記載の本発明にあっては、端末ではICカードに格納されている第1の認証情報を読み出してデータベース装置に送信し、ICカードに格納されている第2の認証情報を読み出してデータベース装置に送信する。

【0014】また、請求項5記載の本発明は、請求項1または2記載の発明において、端末が、前記データ指定情報で指定されるデータへのアクセスを許可された場合、該データ指定情報で指定されるデータに対するデータの変更、追加登録、読み出しを行うことができることを要旨とする。

【0015】請求項5記載の本発明にあっては、端末はデータへのアクセスを許可された場合、該データに対するデータの変更、追加登録、読み出しを行うことができる。更に、請求項6記載の本発明は、端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第1の認証情報を受信して認証し、この認証結果を端末に返送する認証手段と、端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第2の認証情報を受信し、この受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを要旨とする。

【0016】請求項6記載の本発明にあっては、端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第2の認証情報をデータベース装置に送信し、データベース装置は第2の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。

【0017】請求項7記載の本発明は、端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第1の認証情報およびデータアクセス対象を認証する第2の認証情報を受信し、この受信した第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納する格納手段と、端末からデータを指定するデ

ータ指定情報とともに送信されてくる第1の認証情報およびデータアクセス対象情報を受信し、この受信した第1の認証情報で前記格納手段に格納されている第1および第2の認証情報の対を参照し、前記受信したデータアクセス対象が第1の認証情報に対して対として格納されている第2の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを要旨とする。

【0018】請求項7記載の本発明にあっては、端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納し、端末からデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第1および第2の認証情報の対を参照し、データアクセス対象が第2の認証情報で認証されるものであるか否かを判定し、そうである場合、第1、第2の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行なうことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【0019】また、請求項8記載の本発明は、請求項6または7記載の発明において、前記アクセス許可手段が、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを蓄積する蓄積手段を有することを要旨とする。

【0020】請求項8記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス

制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【0021】更に、請求項9記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、端末から送信されるアクセス者を認証する第1の認証情報を受信して認証し、この認証結果を端末に返送し、端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第2の認証情報を受信し、この受信した第2の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するデータベース制御プログラムを記録媒体に記録することを要旨とする。

【0022】請求項9記載の本発明にあっては、端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第2の認証情報をデータベース装置に送信し、データベース装置は第2の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するデータベース制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0023】請求項10記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、端末から送信されるアクセス者を認証する第1の認証情報およびデータアクセス対象を認証する第2の認証情報を受信し、この受信した第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納し、端末からデータを指定するデータ指定情報とともに送信されてくる第1の認証情報およびデータアクセス対象情報を受信し、この受信した第1の認証情報で前記格納されている第1および第2の認証情報の対を参照し、前記受信したデータアクセス対象が第1の認証情報に対して対として格納されている第2の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第2の認証情報で認証されるものである場合、第1および第2の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するデータベース制御プログラムを記録媒体に記録することを要旨とする。

【0024】請求項10記載の本発明にあっては、端末

から第1の認証情報および第2の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証し、第1の認証情報と第2の認証情報を対にして格納し、端末からデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第1および第2の認証情報の対を参照し、データアクセス対象が第2の認証情報で認証されるものであるか否かを判定し、そうである場合、第1、第2の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するデータベース制御プログラムを記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0025】また、請求項11記載の本発明は、請求項9または10記載の発明において、前記アクセスを許可する処理が、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納するデータベース制御プログラムを記録することを要旨とする。

【0026】請求項11記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するデータベース制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0027】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図1は、本発明の一実施形態に係るデータベースアクセス制御方法を実施するICカードを用いたデータベースアクセス制御システムの構成を示すブロック図である。同図に示すデータベースアクセス制御システムは、一例として医療用データベースシステムを構成するものであり、本データベースへのアクセス者である医師によって操作される利用者端末1および該利用者端末1に通信回線5を介して接続されているデータベースシステム7を有する。通信回線5は、例えばAIN回線、ISDN回線、アナログ回線、光ケーブル回線などの様々な種々の通信回線で構成され得るものである。

【0028】利用者端末1は、ICカードリーダ3を有し、このICカードリーダ3に利用者である医師の認証情報などが記憶された医師用のICカードや患者の認証情報などが記憶された患者用のICカードを挿入すると、これらのICカードに記憶された認証情報などの情報はICカードリーダ3で読み取られて、利用者端末1に入力されるようになっている。そして、利用者端末1は、ICカードリーダ3から読み込んだ認証情報などの情報を通信回線5を介してデータベースシステム7に送

信し得るようになっている。また、利用者端末1は、データベースシステム7から送信されるデータを通信回線5を介して受信し、利用者が視覚的に認識し得るように表示する機能を有している。

【0029】データベースシステム7は、通信回線5を介して利用者端末1に接続され、利用者端末1とデータの送受信を行う通信モジュール9、認証処理を行う認証モジュール11、データアクセス制御を行うデータアクセス制御モジュール13、データアクセス管理情報を格納するアクセス管理データベース15、およびデータを格納するデータベース17から構成されている。

【0030】更に詳しくは、通信モジュール9は利用者端末1から受信したデータを認証モジュール11やデータアクセス制御モジュール13へ送信する機能、認証モジュール11やデータアクセス制御モジュール13より受信したデータを利用者端末1へ送信する機能、利用者端末1とデータベースシステム7との接続を行う機能を有する。認証モジュール11は通信モジュール9よりICカードデータを受信する機能、ICカードデータより認証を行う機能、認証結果を通信モジュール9へ送信する機能を有する。

【0031】データアクセス制御モジュール13はアクセス管理データベース15、データベース17と接続されており、通信モジュール9より認証結果やアクセスしたいデータを指定するデータを受信する機能、それらをアクセス管理データベース15と照合する機能、照合結果によってデータベース17よりデータを通信モジュール9へ送信する機能を有する。

【0032】なお、本実施形態では、認証モジュール11をデータベースシステム7がその一部として有するような構成となっているが、認証モジュール11をデータベースシステム7とは別に例えば認証サーバとして設けてもよいものである。

【0033】図2(a)、(b)は、アクセス管理データベース15に格納されているデータ管理テーブルの構成を示す図である。図2(a)に示すデータ管理テーブルは、データ毎にアクセス可能な患者と医師を管理するテーブルであり、データを指定するデータ、すなわちデータ指定情報に対応して、患者を指定するデータおよび医師を指定するデータが登録されている。また、図2(b)に示すデータ管理テーブルは、患者毎にアクセス可能な医師を管理するテーブルであり、患者を指定するデータに対応して医師を指定するデータが登録されている。

【0034】次に、図3～図8に示すフローチャートを参照して、以上のように構成されるデータベースアクセス制御システムの作用について説明する。なお、この説明における前提条件として、ICカードとは、医師、患者が1人1枚以上持っており、ICカードには認証モジュール11で認証するのに十分であるデータが蓄積され

ているものとし、また、医師が特定の目的のためだけにデータにアクセスし、患者データの漏洩を防止するために、患者のデータに医師がアクセスする際には、医師のICカードと患者のICカードを必須とする前提にする。

【0035】まず、図3に示すフローチャートを参照して、医師が利用者端末1を通信回線5を介してデータベースシステム7に接続する方法について説明する。この方法は医師の認証データを通信モジュール9に送信する機能と、医師認証データにより認証を行う機能とに分けられる。

【0036】まず、医師の認証データを通信モジュール9に送信する機能を説明する。医師は利用者端末1でデータベースシステム7へ接続要求を送信する(ステップS11)。通信モジュール9は利用者端末1へ医師認証データ要求を送信する(ステップS13)。利用者端末1は通信モジュール9からの医師認証データ要求を受信して、ディスプレイ上に医師のICカード挿入を促すメッセージを表示する。医師がICカードをICカードリーダに挿入すると(ステップS15)、ICカード内の認証データが通信モジュール9へ送信される(ステップS17)。通信モジュール9への送信は自動的に行つても、医師にボタンなどをクリックさせてもどちらでも構わない。

【0037】医師認証データにより認証を行う機能を説明する。通信モジュール9は利用者端末1から受信した認証データを認証モジュール11に送信する(ステップS19)。認証モジュール11は受信した認証データで認証を行う(ステップS21)。認証結果を通信モジュール9に送信する(ステップS23)。認証結果を判定し(ステップS25)、認証が正しく行われていなければ、通信モジュール9は利用者端末1に接続不可メッセージを送信する(ステップS27)。利用者端末1は接続不可メッセージを受信し、接続ができなかったことをディスプレイに表示し、ICカードを返却する(ステップS29)。認証が正しく行われていれば、通信モジュール9は利用者端末1とデータベースシステム7との接続を行う(ステップS31)。

【0038】利用者端末1がデータベースシステム7に接続されると、医師は利用者端末1からデータベースシステム7に対して新しいデータの入力、既存のデータへのアクセス、主治医の登録または本処理の終了のいずれかを行うことになる(ステップS33)。新しいデータの入力を行う場合には、飛び越し記号Bを介して図4に示す処理に移行し、また既存のデータへのアクセスを行う場合には、飛び越し記号Cを介して図5に示す処理に移行し、主治医の登録を行う場合には、飛び越し記号Dを介して図6に示す処理に移行することになる。

【0039】次に、まず図4に示すフローチャートを参照して、新しいデータの入力、すなわち患者ICカード

の認証を行って、新しい患者データの登録を行う方法について説明する。この方法は患者の認証データを通信モジュールに送信する機能、認証データにより認証を行う機能、認証結果を利用者端末に送信する機能、利用者端末から登録データを送信する機能、データにアクセスさせるためのアクセス管理データを登録する機能、データベースにデータを登録する機能とに分けられる。

【0040】まず、患者の認証データを通信モジュール9に送信する機能を説明する。この場合には、最初に患者のICカードを使用するか否かがチェックされる（ステップS41）。患者のICカードを使用しない場合には、飛び越し記号Dを介して図7および図8に示す処理に移行するが、ここでは患者のICカードを使用する場合について説明する。

【0041】医師は、利用者端末1のディスプレイ上で新しい患者のデータを登録する作業を行うことを指定する。ディスプレイ上で患者ICカードを使用してデータの登録を行う作業を行うことを指定すると、患者のICカード挿入を促すメッセージを表示する。患者ICカードをICカードリーダに挿入すると（ステップS43）、ICカード内の認証データが通信モジュールへ送信される（ステップS45）。通信モジュール9への送信は自動的に行っても、医師や患者にボタンなどをクリックさせてどちらでも構わない。

【0042】患者認証データにより認証を行う機能を説明する。通信モジュール9は利用者端末1から受信した認証データを認証モジュール11に送信する（ステップS47）。認証モジュール11は受信した認証データで認証を行う（ステップS49）。

【0043】次に、認証結果を利用者端末1に送信する機能を説明する。認証モジュール11は認証結果を通信モジュール9に送信する。通信モジュール9は認証結果を判定し（ステップS53）、認証が正しく行われていなければ、通信モジュール9は利用者端末1に登録不可メッセージを送信する（ステップS55）。利用者端末1は登録不可メッセージを受信し、登録できないことをディスプレイに表示し、患者ICカードを返却する（ステップS57）。そして、処理は図3のステップS33に戻る。

【0044】利用者端末1から登録データを送信する機能を説明する。患者認証が正しく行われれば、利用者端末1から認証した患者に関する登録データを通信モジュール9に送信する（ステップS59）。通信モジュール9に送信される登録データはアクセス管理データベース15に登録するデータと、データベース17に登録するデータである。

【0045】データにアクセスさせるためのアクセス管理データを登録する機能を説明する。通信モジュール9はアクセス管理データベース15に登録するデータを送信する（ステップS61）。アクセス管理データベース

15に登録するデータの概念は図2(a)で示すものである。データベース17に登録するデータを指定するデータと一緒に認証した患者を指定するデータと認証した医師を指定するデータをアクセス管理データベース15に登録する（ステップS63）。データベース17に蓄積するデータへのアクセスはここで登録した患者と医師の認証が必須になる。診療上、他の医師にもこのデータへのアクセスを許す必要があれば、同じデータを指定するデータと患者を指定するデータにおいて、他の医師を指定するデータを登録しても構わない。

【0046】データベース17にデータを登録する機能を説明する。利用者端末1から受信したデータをデータベース17に登録する（ステップS65）。登録が終したら、図3のステップS33に戻り、医師の認証完了時の状態に戻る。

【0047】次に、図5に示すフローチャートを参照して、既存のデータへのアクセス、すなわち患者ICカードを使用して、患者データへアクセスする方法を説明する。この方法はアクセスしたいデータを指定する機能、患者の認証データを通信モジュール9に送信する機能、患者認証データにより認証を行う機能、データアクセス制御を行う機能とに分けられる。

【0048】まず、アクセスしたいデータを指定する機能を説明する。利用者端末1とデータベースシステム7とが接続されたら（ステップS31）、医師認証結果よりアクセス管理データベースを検索する（ステップS71）。これは図2(a)で医師を指定するデータと一致するデータを検索するということである。検索した結果を基に、データベース17にて当該医師にアクセスを許すリストを作成し、アクセス可能データリストを通信モジュールへ送信する（ステップS73）。通信モジュール9は受信したアクセス可能データリストを利用者端末1へ送信する（ステップS75）。利用者端末1はアクセス可能データリストを表示する（ステップS77）。このアクセスを許すリストはデータを指定するデータより作成されたデータの一覧であるが、データを選択しやすいように患者でソートするなどの工夫がしてあっても構わない。

【0049】医師がアクセスしたいデータがなければステップS33に戻って、医師の認証完了時の状態に戻る（ステップS77のNO）。医師がアクセスしたいデータがあれば、そのデータをクリックして通信モジュール9へアクセスしたいデータを指定するデータを送信する（ステップS81）。

【0050】次に、患者の認証データを通信モジュール9に送信する機能を説明する。通信モジュール9はアクセスしたいデータを指定するデータを受信後、患者認証データ要求を利用者端末1に送信する（ステップS83）。利用者端末1は患者認証データ要求を通信モジュールより受信して、ディスプレイ上に患者ICカード挿

入を促すメッセージを表示する。医師は、医師ICカードを取り出し、患者ICカードをICカードリーダ3に挿入する（ステップS85）。患者認証データを通信モジュール9に送信する（ステップS87）。通信モジュール9への患者認証データの送信は自動的に行っても医師によるボタンのクリックなどで行ってもどちらでも構わない。

【0051】患者認証データにより認証を行う機能を説明する。通信モジュール9は利用者端末1より受信した患者認証データを認証モジュール11へ送信する（ステップS89）。認証モジュール11は受信した認証データで認証を行う（ステップS91）。認証結果を通信モジュールに送信する（ステップS93）。通信モジュール9は、認証結果を判定し（ステップS95）、認証が正しく行われていなければ、通信モジュール9は利用者端末1にアクセス不可メッセージを送信する（ステップS97）。利用者端末1はアクセス不可メッセージを受信し（ステップS99）、データにアクセスできなかつことをディスプレイに表示し、ICカードを返却する。ICカード返却後、ステップS77に戻り、当該医師がアクセス可能なアクセス可能データリストを表示し、以下同様の処理を行う。

【0052】認証が正しく行われていれば、通信モジュール9はデータアクセス制御モジュール13にアクセスしたいデータを指定するデータと医師認証結果、患者認証結果を送信する。

【0053】次に、データアクセス制御を行う機能を説明する。アクセス管理データベース15により医師認証結果、患者認証結果が指定されたデータへのアクセス条件として十分であるかどうかの照合を行う（ステップS101）。これは図2(a)でデータを指定したデータと一致するデータを検索した時、患者を指定するデータと医師を指定するデータがそれぞれの認証結果と一致するかどうか照合するということである。照合の結果、アクセス不可であれば、アクセス管理データベース15は通信モジュール9へアクセス不可メッセージを送信する。通信モジュール9は利用者端末1にアクセス不可メッセージを送信する（ステップS97）。利用者端末1はアクセス不可メッセージを受信し、データにアクセスできなかつことをディスプレイに表示し、ICカードを返却する。ICカード返却後、ステップS77に戻り、当該医師がアクセス可能なアクセス可能データリストを表示し、以下同様の処理を行う。

【0054】照合の結果、アクセス可能であれば、アクセス管理データベース15はデータベース17へ当該データを通信モジュール9へ送信するように要求をかける。データベース17は当該データを通信モジュール9へ送信する（ステップS103）。通信モジュール9は当該データを利用者端末1へ送信する（ステップS105）。利用者端末1は受信した当該患者データをディス

プレイに表示する（ステップS107）。患者データを使用して作業を行った後には当該患者データの表示を終了し、ステップS77に戻り、医師がアクセス可能データリストを表示する。

【0055】上述した説明では、医師が特定の目的のためだけにデータにアクセスし、患者データの漏洩を防止するために、患者のデータに医師がアクセスする際には、医師のICカードと患者のICカードを必須とする前提にした。しかし、実際の医療業務では、主治医は患者帰宅後に患者データへのアクセスを行うことが求められ、患者ICカードが無いために患者のデータへのアクセスができないという問題が生じる。また、他院により入力された患者のデータに主治医であるにもかかわらずアクセスできないという問題が生じる。その問題を解決するためには、患者のICカードを必須としないデータの登録やアクセスを可能にするという前提に基づいた方式が必要である。しかし、どの医師に対しても無条件に患者データへのアクセスを許すのでは患者データ漏洩時の責任の明確化ができない。そのために、患者が主治医と指定した医師のみに患者のデータを患者ICカード無しでも登録したりアクセスしたりできるようにする処理について図6を参照して説明する。

【0056】図6に示すフローチャートを参照して、主治医を登録する処理、すなわち患者ICカードの認証を行って、患者に主治医を登録する方法を説明する。なお、この方法では、図3に示した医師の認証結果を基にして利用者端末1とデータベースシステム7との接続を行うまでの処理は図3に示す処理と同じである。また、この方法は患者の認証データを通信モジュール9に送信する機能、認証データにより認証を行う機能、認証結果を利用者端末1に送信する機能、利用者端末1から登録する患者の主治医データを送信する機能、アクセス管理データベースに患者の主治医を登録する機能とに分けられる。

【0057】まず、患者の認証データを通信モジュール9に送信する機能を説明する。ディスプレイ上で患者に主治医を登録する作業を行うことを指定する。患者のICカード挿入を促すメッセージを表示する。患者ICカードをICカードリーダ3に挿入すると（ステップS111）、ICカード内の認証データが通信モジュールへ送信される（ステップS113）。通信モジュール9への送信は自動的に行っても、医師や患者にボタンなどをクリックさせてもどちらでも構わない。

【0058】患者認証データにより認証を行う機能を説明する。通信モジュール9は利用者端末1から受信した認証データを認証モジュール11に送信する（ステップS15）。認証モジュール11は受信した認証データで認証を行う（ステップS117）。

【0059】認証結果を利用者端末1に送信する機能を説明する。認証モジュール11は認証結果を通信モジ

ール9に送信する（ステップS119）。通信モジュール9は、認証結果を判定し（ステップS121）、認証が正しく行われていなければ、通信モジュール9は利用者端末1に登録不可メッセージを送信する（ステップS123）。利用者端末1は登録不可メッセージを受信し（ステップS125）、登録できることをディスプレイに表示し、患者ICカードを返却する。そして、ステップS33に戻る。

【0060】利用者端末1から登録する患者の主治医データを送信する機能を説明する。患者認証が正しく行われれば、利用者端末1からデータベースシステム7に接続した医師を認証した患者の主治医として登録する登録データを通信モジュール9に送信する（ステップS127）。

【0061】アクセス管理データベースに患者の主治医を登録する機能を説明する。通信モジュール9はアクセス管理データベース15に登録するデータを送信する（ステップS129）。アクセス管理データベース15に登録するデータの概念は図2（b）で示すものであり、患者を指定するデータについて、患者が主治医として認めた医師を指定するデータを登録する（ステップS131）。データ登録後、ステップS33に戻り、医師の認証完了時の状態に戻る。

【0062】次に、図7に示すフローチャートを参照して、患者のICカードを使用しないで、医師の主治医の権限で新しい患者データを登録する方法について説明する。この方法は利用者端末1から登録データを送信する機能、アクセス管理データベース15で認証された医師が患者データの主治医であるかのチェックを行う機能、登録するデータにアクセスさせるためのアクセス管理データを登録する機能、データベース17にデータを登録する機能とに分けられる。

【0063】まず、利用者端末1から登録データを送信する機能を説明する。利用者端末1からデータベース17に登録したいデータとそのデータへのアクセス管理のためのデータを通信モジュール9に送信する（ステップS141）。通信モジュール9は利用者端末1から受信したデータをアクセス管理データベース15へ送信する（ステップS143）。

【0064】アクセス管理データベース15で認証された医師が患者データの主治医であるかのチェックを行う機能を説明する。アクセス管理データベース15を検索することにより、登録しようとしている患者の主治医が認証された医師であるかどうか照合を行う（ステップS145）。これは図2（b）で登録しようとしている患者を指定するデータに対して認証された医師を指定するデータが登録されているか否かについての検索を行うことである。照合の結果、医師が患者の主治医として登録されていなければ通信モジュールに登録不可メッセージを送信する。通信モジュール9は登録不可メッセージを

利用者端末1に送信する（ステップS147）。利用者端末1は登録不可メッセージを受信し、登録できないことをディスプレイに表示し（ステップS149）、医師の認証完了時の状態であるステップS33に戻る。

【0065】次に、登録するデータにアクセスさせるためのアクセス管理データを登録する機能を説明する。アクセス管理データベース15に登録するデータの概念は図2（a）で示すものであり、データベース17に登録するデータを指定するデータと一緒に患者を指定するデータと認証した医師を指定するデータをアクセス管理データベース15に登録する（ステップS151）。データベース17に蓄積するデータへのアクセスはここで登録した患者と医師の認証は必須になる。診療上、他の医師にもこのデータへのアクセスを許す必要があれば、同じデータを指定するデータと患者を指定するデータにおいて、他の医師を指定するデータを登録しても構わない。

【0066】データベース17にデータを登録する機能を説明する。利用者端末1から受信したデータをデータベース17に登録する（ステップS153）。登録が終了したら、医師の認証完了時の状態であるステップS33に戻る。

【0067】次に、図8に示すフローチャートを参照して、患者のICカードを使用しないで、医師の主治医の権限で患者データにアクセスする方法について説明する。この方法は、利用者端末1から患者を指定するデータを送信する機能、アクセス管理データベース15で認証された医師が患者の主治医であるかのチェックを行う機能、アクセス可能データリストを利用者端末1に送信する機能、利用者端末1からアクセスしたいデータを指定するデータを送信する機能、データベース17が利用者端末1へデータを送信する機能とに分けられる。

【0068】まず、利用者端末1から患者を指定するデータを送信する機能を説明する。患者を指定したデータの参照を行うか否かの判定を行い（ステップS161）、参照しない場合は、ここで医師の認証完了時の状態であるステップS33に戻る。患者を指定したデータの参照を行う場合は、患者を指定するデータと医師の認証結果をアクセス管理データベース15に送信する（ステップS163）。

【0069】次に、アクセス管理データベース15で認証された医師が患者の主治医であるかのチェックを行う機能を説明する。アクセス管理データベース15を検索することにより、指定した患者の主治医が認証された医師であるかどうか照合を行う（ステップS165）。これは図2（b）で指定された患者を指定するデータに対して認証された医師を指定するデータが登録されているか検索を行うことである。照合の結果、医師が患者の主治医として登録されていなければ通信モジュール9にアクセス不可メッセージを送信する。通信モジュール9は

アクセス不可メッセージを利用者端末1に送信する(ステップS167)。利用者端末1はアクセス不可メッセージを受信し(ステップS169)、アクセスできないことをディスプレイに表示し、医師の認証完了時の状態であるステップS33に戻る。

【0070】アクセス可能データリストを利用者端末1に送信する機能を説明する。患者に対して医師が主治医として登録されれば、患者を指定するデータによりデータベース17を検索する。これは、図2(a)で患者を指定するデータと一致するデータを検索して、データベース17よりリストを作成してもいいし、直接データベース17を患者を指定するデータで検索しても構わない。検索した結果を基に、データベース17にて当該医師にアクセスを許すリストを作成し、アクセス可能データリストを通信モジュール9へ送信する(ステップS171)。通信モジュール9は受信したアクセス可能データリストを利用者端末1へ送信する(ステップS173)。

【0071】利用者端末1からアクセスしたいデータを指定するデータを送信する機能を説明する。利用者端末1はアクセス可能データリストを表示する(ステップS175)。医師がアクセスしたいデータがなければ、医師の認証完了時の状態であるステップS33に戻る。医師がアクセスしたいデータがあれば、そのデータをクリックして送信する(ステップS177, S179)。

【0072】データベース17が利用者端末1へデータを送信する機能を説明する。データベース17は利用者端末1より受信したアクセスしたいデータを指定するデータによりデータベース17を検索し、当該データを通信モジュール9へ送信する(ステップS181)。通信モジュール9はデータベース17より受信したデータを利用者端末1へ送信する(ステップS183)。利用者端末1は受信したデータをディスプレイに表示する(ステップS185)。患者データを使用して作業を行った後には当該患者データの表示を終了し、ステップS175に戻って、医師がアクセス可能データリストを表示する。

【0073】なお、上記実施形態のデータベースアクセス制御方法の処理手順をプログラムとして記録媒体に記録して、この記録媒体をコンピュータシステムに組み込むとともに、該記録媒体に記録されたプログラムをコンピュータシステムにダウンロードまたはインストールし、該プログラムでコンピュータシステムを作動させることにより、データベースアクセス制御方法を実施するデータベースアクセス制御システムとして機能させることができることは勿論であり、このような記録媒体を用いることにより、その流通性を高めることができるものである。

【0074】

【発明の効果】以上説明したように、本発明によれば、

端末から第1の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第2の認証情報をデータベース装置に送信し、データベース装置は第2の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するので、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。更に、患者毎にアクセス可能な医師を管理することにより、例えば患者が主治医と見なした医師のみに対して他の医療設備などによって入力された患者データへのアクセス、患者不在時の患者データへのアクセスを可能にすることができる。これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行うことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【0075】また、本発明によれば、端末から第1および第2の認証情報をデータベース装置に送信し、データベース装置は第1の認証情報を認証して、第1および第2の認証情報を対にして格納し、端末からデータ指定情報とともに第1の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は第1および第2の認証情報の対を参照し、データアクセス対象が第2の認証情報で認証されるものである場合、データ指定情報で指定されるデータへのアクセスの可否を判定するので、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、症例検索など医療の質の向上のために患者データを有効活用することができる。更に、患者毎にアクセス可能な医師を管理することにより、例えば患者が主治医と見なした医師のみに対して他の医療設備などによって入力された患者データへのアクセス、患者不在時の患者データへのアクセスを可能にすることができる。これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行うことができるとともに、また他の病院により診療や投薬の情報も主治医がチェックで

きるようになる。

【0076】更に、本発明によれば、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス制御をデータ毎に行なうことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るデータベースアクセス制御方法を実施するICカードを用いたデータベースアクセス制御システムの構成を示すブロック図である。

【図2】図1に示す実施形態に使用されているアクセス管理データベースに格納されているデータ管理テーブルの構成を示す図である。

【図3】図1に示す実施形態において医師が利用者端末を通信回線を介してデータベースシステムに接続する方法を示すフローチャートである。

【図4】図1に示す実施形態において患者ICカードの認証を行って、新しい患者データの登録を行う方法を示すフローチャートである。

すフローチャートである。

【図5】図1に示す実施形態において患者ICカードを使用して、患者データへアクセスする方法を示すフローチャートである。

【図6】図1に示す実施形態において患者ICカードの認証を行って、患者に主治医を登録する方法を示すフローチャートである。

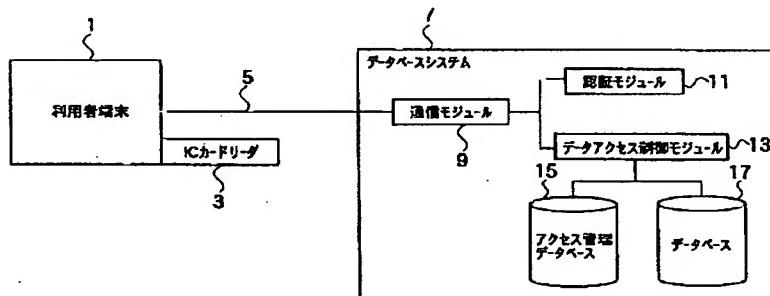
【図7】図1に示す実施形態において患者のICカードを使用しないで、医師の主治医の権限で新しい患者データを登録する方法を示すフローチャートである。

【図8】図1に示す実施形態において患者のICカードを使用しないで、医師の主治医の権限で患者データをアクセスする方法を示すフローチャートである。

【符号の説明】

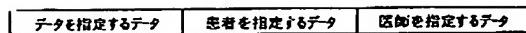
- 1 利用者端末
- 3 ICカードリーダ
- 5 通信回線
- 7 データベースシステム
- 9 通信モジュール
- 11 認証モジュール
- 13 データアクセス制御モジュール
- 15 アクセス管理データベース
- 17 データベース

【図1】



【図2】

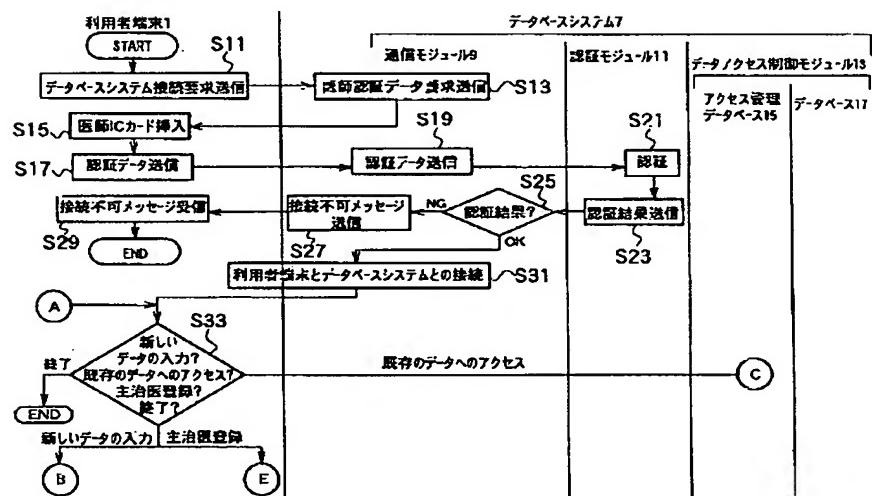
(a)



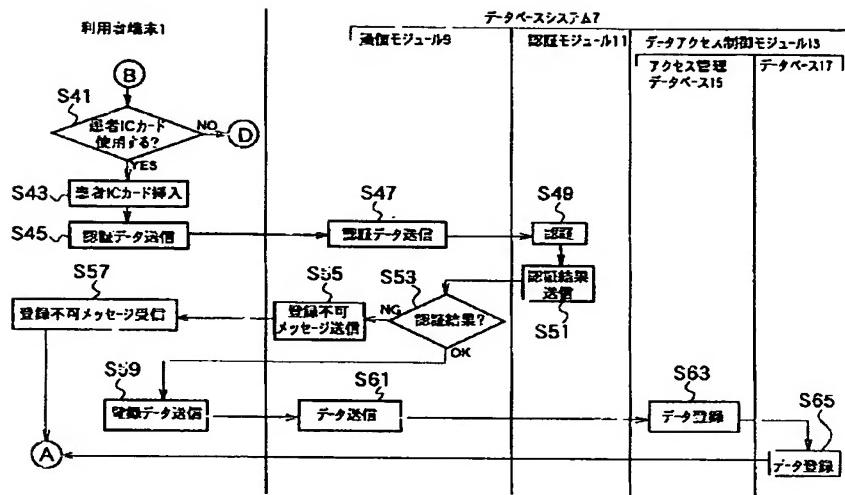
(b)



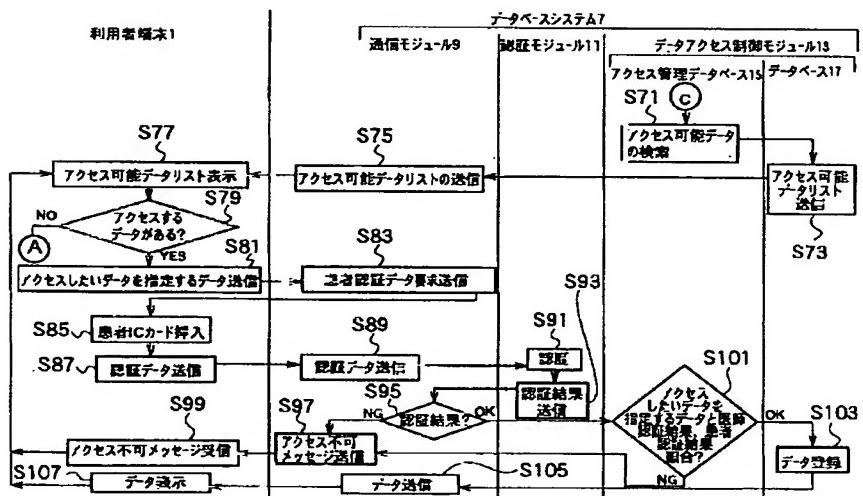
【図3】



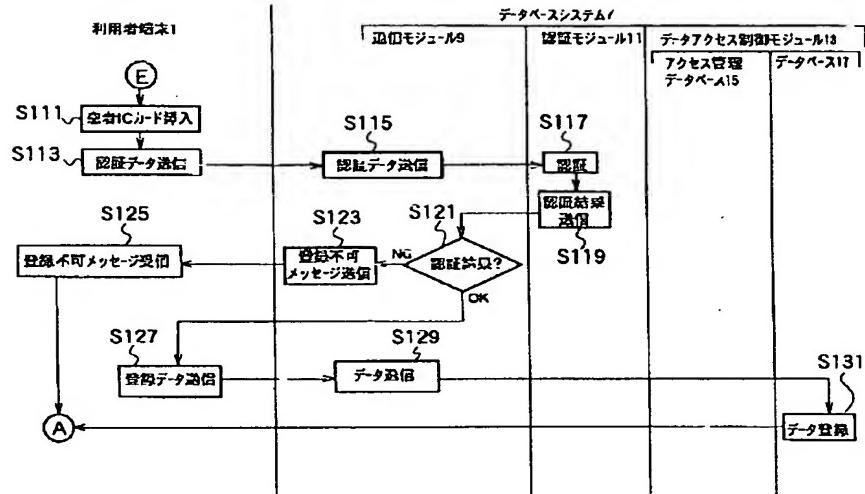
【図4】



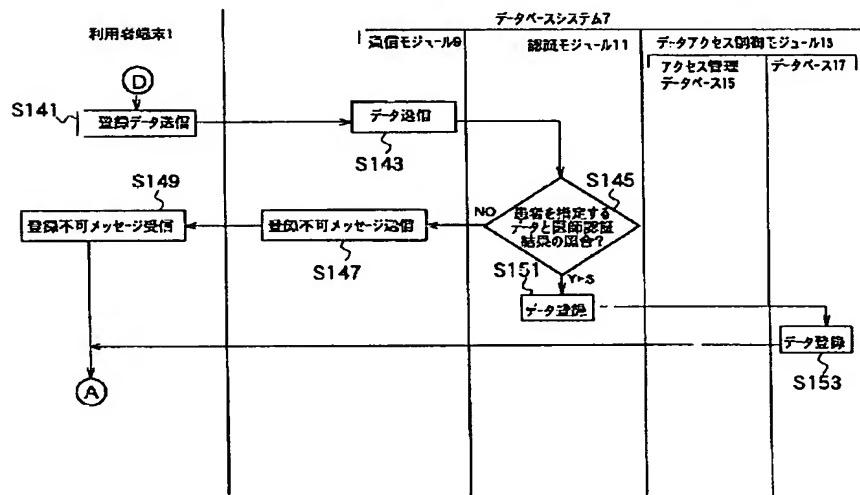
【図5】



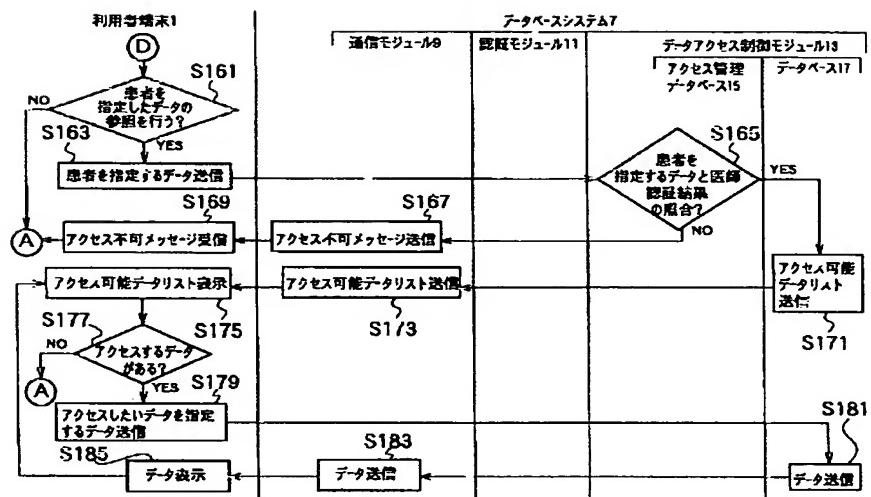
【図6】



【図7】



【図8】



フロントページの続き

(72) 発明者 坪井 俊明
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

(72) 発明者 中村 能章
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

(72) 発明者 橋本 聰
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

(72) 発明者 澤地 守
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

F ターム(参考) 5B017 AA01 AA04 BA05 BB02 CA16
 5B075 KK43 KK54 KK63 PP06 PP13
 PQ02 PQ46 UU26

5B082 EA12 GA16 GC04
 5B085 AE06 AE12 AE23